AFFIDAVIT OF BRIAN J. SOLECKI

I, Brian J. Solecki, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I am a Special Agent with the United States Department of Defense, Defense Criminal Investigative Service (DCIS) and have been employed in that capacity since August 2012. Prior to my current assignment I served as a Special Agent with the Air Force Office of Special Investigations (AFOSI) from 2004 to 2012 where I received formal training at the Federal Law Enforcement Training Center. I am currently assigned to the DCIS Northeast Field Office, Boston Resident Agency, Boston, MA. My current assignment includes investigating violations of the Export Administration Act of 1979, 50 U.S.C. §§ 2401-2420, and the International Emergency Economic Powers Act, 50 U.S.C. §§ 1701 et seq., and relevant regulations. Based on my training and experience, I am familiar with the means by which individuals and/or groups attempt to illegally export weapons, technology, and other controlled commodities.

2. As set forth herein, DCIS is participating with Homeland Security Investigations (HSI); Department of Commerce, Office of Export Enforcement (DOC/OEE) and Naval Criminal Investigative Service (NCIS) in the investigation of EZZAT KHODADADI and other entities associated with him, to include organizations known as BEHFONOUN ZARRIN CUT COMPANY and NEW MIRSAL CO., LLC for conspiring to export goods from the United States to the Islamic Republic Iran without a license, in violation of the International Emergency Economic Powers Act (IEEPA), 50 U.S.C. § 1705, and Iranian Transaction Regulations, 31 C.F.R. §§ 560. It is believed that EZZAT KHODADADI and

BEHFONOUN ZARRIN CUT COMPANY are located in Iran while NEW MIRSAL CO., LLC is located in the United Arab Emirates (UAE).

3. I am submitting this affidavit in support of an Application for a Search Warrant to search records and other information (including the contents of communications) associated with certain accounts, specifically **ghazaei.ah@gmail.com** which is stored at premises owned, maintained, controlled, or operated by Google, Inc. ("Google"), an e-mail provider headquartered at 1600 Amphitheatre Parkway, Mountain View, CA 94043. The information to be searched is described in the following paragraphs and in Attachment A.

4. Based on my training and experience, and the facts set forth in this affidavit, there is probable cause to believe violations of the International Emergency Economic Powers Act (IEEPA), 50 U.S.C. § 1705, and Iranian Transaction Regulations, 31 C.F.R. §§ 560 have been committed by these and other unknown targets/suspects. There is also probable cause to believe that records and other information associated with e-mail account **ghazaei.ah@gmail.com** as described in Attachment A, contain evidence, fruits, and/or instrumentalities of various violations of the International Emergency Economic Powers Act (IEEPA), 50 U.S.C. § 1705, and Iranian Transaction Regulations, 31 C.F.R. §§ 560. Accordingly, there is probable cause to search the information described in Attachment A for evidence, fruits, and/or instrumentalities of these crimes, as described in Attachment B. This affidavit is made in support of an Application for a Search Warrant pursuant to Title 18, United States Code, Sections 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), to compel Google, a provider of electronic communication and remote computing services, to provide certain items as set forth in Attachment B, Part I, hereto, and for the

government to search and to seize certain items as set forth in Attachment B, Part II, hereto.

5. The facts set forth in this affidavit are based upon my personal observations, my review of documents and computer records, my training and experience, and information obtained from other agents and witnesses, including other law enforcement agents. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge of the investigation into this matter.

II. PROBABLE CAUSE

6. The affiant believes there is probable cause that violations of the International Emergency Economic Powers Act (IEEPA), 50 U.S.C. § 1705, and Iranian Transaction Regulations, 31 C.F.R. §§ 560 and have been committed by these and other targets and that evidence, instrumentalities, or fruits of criminal activity will be found in a search of computer servers hosted at Google for the following reasons.

7. In November 2012, KVH Industries, a U.S. based manufacturer of military and commercial navigation equipment received an unsolicited email by an individual utilizing ebpkh9073@gmail.com who identified himself as EZZAT KHODADADI. In said email, KHODADADI requested pricing information for approximately twenty-five C100 Compass Engines, an industrial grade compass module with a wide variety of military and commercial applications. KHODADADI initially revealed the C100 Compass Engines were to be utilized for meteorological buoys at sea and requested the order be shipped to the UAE.

8. The affiant observed subsequent email communications in which KVH determined the final destination of the compasses was to be Iran and informed KHODADADI they could not authorize the sale and shipment of the C100 Compass Engines believing their ultimate destination was Iran. KHODADAI replied the C100 Compass Engines could be shipped to his company in the UAE and upon receipt he would arrange for trans-shipment to Iran. KVH advised KHODADADI the trans-shipment of C100 Compass Engines from the UAE to Iran was also prohibited.[1] As a result, KHODADADI requested the assistance of KVH in circumventing U.S. export laws and facilitating the shipment of the C100 Compass Engines to Iran.

9. Subsequent to the aforementioned email communications between Khodadadi and KVH, I have reviewed a series of email communications between Khodadadi or his associates and a representative of a New Hampshire based U.S. Company regarding the shipment of the

---

[1] As a result of Iran's support for international terrorism and its aggressive actions against non-belligerent shipping in the Persian Gulf, President Reagan, on October 29, 1987, issued Executive Order 12613 imposing a new import embargo on Iranian-origin goods and services. Section 505 of the International Security and Development Cooperation Act of 1985 ("ISDCA") was utilized as the statutory authority for the embargo, which gave rise to the Iranian Transactions Regulations, Title 31, Part 560 of the U.S. Code of Federal Regulations (the "ITR"). On May 6, 1995, President Clinton signed Executive Order 12959, pursuant to the International Emergency Economic Powers Act ("IEEPA") as well as the ISDCA, substantially tightening sanctions against Iran. On August 19, 1997, the President signed Executive Order 13059 clarifying Executive Orders 12957 and 12959 confirming that virtually all trade and investment activities with Iran by U.S. persons, wherever located, are prohibited.

In general, unless licensed by Office of Foreign Assets Control of the Department of Treasury, goods, technology, or services may not be exported, reexported, sold or supplied, directly or indirectly, from the United States or by a U.S. person, wherever located, to Iran or the Government of Iran. The ban on providing services includes any brokering function from the United States or by U.S. persons, wherever located. For example, a U.S. person, wherever located, or any person acting within the United States, may not broker offshore transactions that benefit Iran or the Government of Iran, including sales of foreign goods or arranging for third-country financing or guarantees.

In general, a person may not export from the U.S. any goods, technology or services, if that person knows or has reason to know such items are intended specifically for supply, transshipment or reexportation to Iran. Further, such exportation is prohibited if the exporter knows or has reason to know the U.S. items are intended specifically for use in the production of, for commingling with, or for incorporation into goods, technology or services to be directly or indirectly supplied, transshipped or reexported exclusively or predominately to Iran or the Government of Iran.

C100 Compass Engines. The New Hampshire company's representative was located in New Hampshire when he transmitted and accessed those emails. The following are descriptions of some of those email communications:

10. The affiant observed an email communication in which the writer utilizing email address psa.sks10@yahoo.com identifies himself as PEJMAN SADEGHI, the brother of EZZAT KHODADADI and related he was utilizing a Yahoo email account as their Gmail account (ebpkh9073@gmail.com) was not working. As such, from April 2013 to the present, psa.sks10@yahoo.com has been serving as the primary method of communication being utilized to illegally procure the C100 Compass Engines in violation of U.S. law.

11. The affiant observed an email communication in which SADEGHI utilizing email address psa.sks10@yahoo.com relates that he has an associate who is currently residing in Germany who could bring the C100 Compass Engines to Iran. SADEGHI inquires if the C100 Compass Engines could be shipped to Germany and if so, he will provide the contact information for his associate.

12. The affiant observed an email communication in which SADEGHI utilizing email address psa.sks10@yahoo.com inquires if he specifies an end user in Germany, can the C100 Compass Engines be shipped via FedEx, DHL or TNT to Germany. SADEGHI relates they may be able to circumvent additional risk by specifying his associate in Germany as the end user for the C100 Compass Engines. Additionally, SADEGHI suggests his associate in Germany may be able to travel to another location and physically receive the C100 Compass Engines for ultimate delivery to Iran.

13. The affiant observed multiple email communications in which SADEGHI utilizing email address psa.sks10@yahoo.com suggests again that his associate in Germany may be able to

travel to another location and physically receive the C100 Compass Engines for ultimate delivery to Iran.

14. The affiant observed an email communication in which SADEGHI utilizing email address psa.sks10@yahoo.com provides an email address of ghazaei.ah@gmail.com as the contact email address for his associate in Germany.

15. The affiant observed an email communication from email address ghazaei.ah@gmail.com by an individual who identifies himself as AMIRHOSSEIN GHAZAEI who claims to be currently residing in Germany. GHAZAEI relates that "regarding to the deal about the products you are going to sell to your customer in Iran" he is available to discuss in greater detail and provides a contact cell phone number of 0049 157 3164 3747 and a contact email address of ghazaei.ah@gmail.com.

16. Open source searches conducted on ghazaei.ah@gmail.com identified it as the contact email address for an individual identified as AMIR HOSSEIN GHAZAEI on the LinkedIn website from Germany. According to the website, GHAZAEI identifies himself as a Master of Science (MSC) student in Production Engineering from the Bielefeld area of Germany who is seeking new business opportunities. Additionally, the website indicates GHAZAEI earned a Bachelor of Science degree in Industrial Engineering from Isfahan University of Technology, Isfahan, Iran in 2008 and until 2012 was employed as a Project Manager Assistant at the Research and Development Department of the Entekhab Group, an Isfahan, Iran based firm which manufactures and sells home appliances and consumer electronics.

III. TECHNICAL BACKGROUND

17. In my training and experience, I have learned that Google provides a variety of on-line services, including electronic mail ("e-mail") access, to the general public. Google allows subscribers to obtain e-mail accounts at the domain name google.com like e-mail account **ghazaei.ah@gmail.com** listed in Attachment A. Subscribers obtain an account by registering with Google. During the registration process, Google asks subscribers to provide basic personal information. Therefore, the computers of Google are likely to contain stored electronic communications (including retrieved and unretrieved e-mail for Google subscribers) and information concerning subscribers and their use of Google services, such as account access information, e-mail transaction information, and account application information.

1. In general, an e-mail that is sent to a Google subscriber is stored in the subscriber's "mail box" on Google servers until the subscriber deletes the e-mail. If the subscriber does not delete the message, the message can remain on a Google server indefinitely.
2. When the subscriber sends an e-mail, it is initiated at the user's computer, transferred via the Internet to Google's servers, and then transmitted to its end destination. Google often saves a copy of the e-mail sent. Unless the sender of the e-mail specifically deletes the e-mail from the Google server, the e-mail can remain on a Google server indefinitely.
3. A sent or received e-mail typically includes the content of the message, source and destination addresses, the date and time at which the e-mail was sent, and the size and length of the e-mail. If an e-mail user writes a draft message but does not send it, that message may also be saved by Google but may not include all of these categories of data.

4. A Google subscriber can also store files, including e-mails, address books, contact or buddy lists, calendar data, pictures, and other files, on servers maintained and/or owned by Google.

5. Subscribers to Google might not store on their home computers copies of the e-mails stored in their Google account. This is particularly true when they access their Google account through the web, or if they do not wish to maintain particular e-mails or files in their residence.

6. In general, e-mail providers like Google ask each of their subscribers to provide certain personal identifying information when registering for an e-mail account. This information can include the subscriber’s full name, physical address, telephone numbers and other identifiers, alternative e-mail addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number).

7. E-mail providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (i.e., session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via Google’s website), and other log files that reflect usage of the account. In addition, e-mail providers often have records of the Internet Protocol address (“IP address”) used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the e-mail account.

8. In some cases, e-mail account users will communicate directly with an e-mail service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. E-mail providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well records of any actions taken by the provider or user as a result of the communications.

9. In my training and experience, evidence of who was using an e-mail account may be found in address books, contact or buddy lists, e-mail in the account, and attachments to e-mails, including pictures and files.

IV. RELEVANT FEDERAL OFFENSES

10. Based upon the information above, your affiant believes that there is probable cause to believe that on the computer systems owned, maintained, and operated by Google, as described above, there exists evidence, fruits, and/or instrumentalities of that violations of the International Emergency Economic Powers Act (IEEPA), 50 U.S.C. § 1705, and Iranian Transaction Regulations, 31 C.F.R. §§ 560, allowing agents to seize records and other information (including content of communications) stored on servers being maintained by Google for the account and files associated with the e-mail account**:** **ghazaei.ah@gmail.com.**

V. LEGAL AUTHORITY AND INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

11. If issued, I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require Google to disclose to the government copies of the records and other information (including the content of communications) located at the premises described in Attachment A ("Place to Be Searched") and particularly described in Attachment B, Part I ("Information to Be Disclosed by Google"). Upon receipt of the information described in Part I of Attachment B, government-authorized persons will review that information to locate the items described in Part II of Attachment B ("Information to Be Seized by the Government").

12. The government may obtain internet and e-mail content and subscriber information from a third party by obtaining a search warrant. 18 U.S.C. §§ 2703(a), 2703(c)(1)(A). Any court with jurisdiction over the offense under investigation may issue a § 2703 warrant, regardless of the location of the server where information will be searched. 18 U.S.C. § 2703(b)(1)(A). Furthermore, unlike Rule 41 search warrants, a § 2703 warrant does not require an officer to be present for service or execution of the search warrant. 18 U.S.C. § 2703(g).

13. If the government obtains a search warrant, there is no requirement that the third party give notice to the subscriber. 18 U.S.C. §§ 2703(b)(1)(A), and (c)(3).

VI. CONCLUSION

14. Based on my training and experience, and the facts as set forth in this affidavit, I submit that there is probable cause to believe that EZZAT KHODADADI and other entities associated with him, to include organizations known as BEHFONOUN ZARRIN CUT COMPANY and NEW MIRSAL CO., LLC and other entities associated with him, to include AMIRHOSSEIN GHAZAEI have committed violations of the International Emergency Economic Powers Act (IEEPA), 50 U.S.C. § 1705, and Iranian Transaction Regulations, 31 C.F.R. §§ 560. Based on my training and experience, and the facts as set forth in this affidavit, there is probable cause to believe that computer systems owned or operated by or in the control of Google, headquartered at 1600 Amphitheater Way, Mountain View, CA 94043, contain evidence, fruits, and instrumentalities of the crimes identified above. Accordingly, a Search Warrant is requested.

15. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A).

/s/ Brian J. Solecki
Special Agent Brian J. Solecki
Defense Criminal Investigative Service

Subscribed and sworn to before me
This 20th day of November, 2013

____

Landya B. McCafferty
United States Magistrate Judge

ATTACHMENT A

Place to Be Searched

This warrant applies to information associated with the e-mail account **ghazaei.ah@gmail.com** that is stored at premises owned, maintained, controlled, or operated by Google, Inc., an e-mail provider headquartered at 1600 Amphitheater Way, Mountain View, CA 94043.

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Google

To the extent that the information described in Attachment A is within the possession, custody, or control of Google, Google is required to disclose the following information to the government for each account or identifier listed in Attachment A, and to the extent it is dated during, or pertaining to the period August 1, 2013 to the present:

a. The contents of all e-mails stored in the account(s), including copies of e-mails sent to and from the account(s), draft e-mails, the source and destination addresses associated with each e-mail; the date and time at which each e-mail was sent, and the size and length of each e-mail;

b. All records or other information regarding the identification of the account(s), to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account(s) was created, the length of service, the types of service utilized, the IP address used to register the account(s), log-in IP addresses associated with session times and dates, account(s) status, alternative e-mail addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);

c. All records or other information stored by an individual using the account(s), including address books, contact and buddy lists, calendar data, pictures, and files;

d. All records pertaining to communications between Google, Inc. and any person regarding the account(s), including contacts with support services and records of actions taken.

II. Information to be seized by the government

All information described above in Section I that constitutes evidence, fruits, and/or instrumentalities of the International Emergency Economic Powers Act (IEEPA), 50 U.S.C. § 1705, and Iranian Transaction Regulations, 31 C.F.R. §§ 560, including, for the account(s) or identifier(s) listed on Attachment A, information relating to the following matters:

1. Electronic mail and other content identifying in any manner the user(s) of the email account.
2. Electronic mail and other content relating to orders or potential orders for U.S. defense articles or defense services and the end-user or potential use for those items or services.
3. Electronic mail and other content referring in any manner to, or reflecting, any transaction or prospective transaction in violation of the Arms Export Control Act, 22 U.S.C. §§2778(b)(2) and 2778(c), the International Traffic in Arms Regulations, 22C.F.R. §§121.1, 123.1, and 127.1, 18 U.S.C. §554(a) (Smuggling), 18 U.S.C. §371 (Conspiracy), 50 U.S.C. §1705 (U.S. Embargo Against Iran)
4. All of the transactional records described in Section II(B)